

**ITU-T Kaleidoscope Conference
Innovations in NGN**

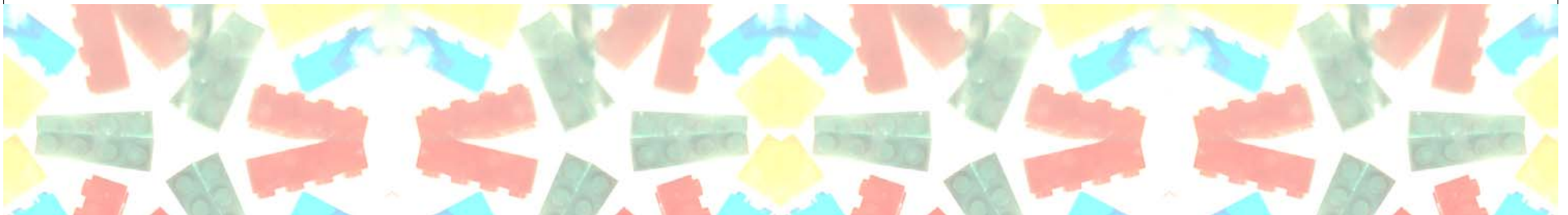
OVERLAY PRIVATE IP ADDRESS NETWORKS OVER WIDE AREA ETHERNET

L.N.Bui, Y.Kawahara, T.Asami

Asami Laboratory, The University of Tokyo

M.Tatipamula

Strategy and planning, Juniper Networks



Outline

1. Introduction
2. Research purpose
3. Proposal
4. 2 proposed methods
 1. MIP+PPPoE
 2. MIP+VLAN
5. Evaluation

1. Introduction

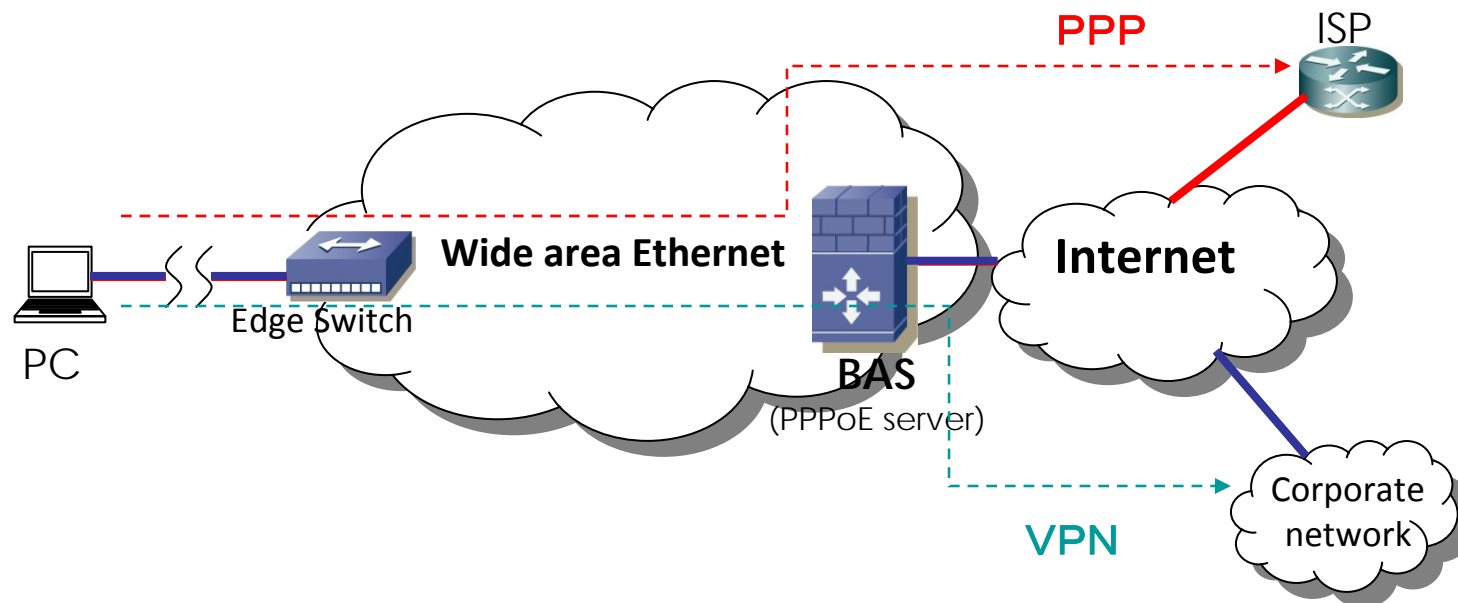
- The typical method to remote access to corporate network is PPP+VPN
 - A mobile node belongs to two layer 3 administration domains (ISP and corporate network)
 - Disadvantages :
 - Cannot prevent malicious activities caused by the use of mobile node outside of the corporation.
 - The inconvenience for users working outside of the corporation.
- Many of corporate networks use private IP address.
- Wide area Ethernet services have become popular but most of the VLAN configuration is set up manually.

2. Research purpose

- Overlay private IP address networks over Wide area Ethernet with low management cost.
 - Sub goals:
 - Unify remote access to one layer 3 administration domain and one layer 2 administration domain.
 - Unify the layer 2 access to the carrier and layer 3 access to the corporate network
 - Advantages :
 - A mobile node which belongs to the corporation is always under its security policy.
 - The access to corporate network is unchanged at outside or inside of the corporation

2. Research purpose

- Replace PPP+VPN method with a better security and lower management cost protocol

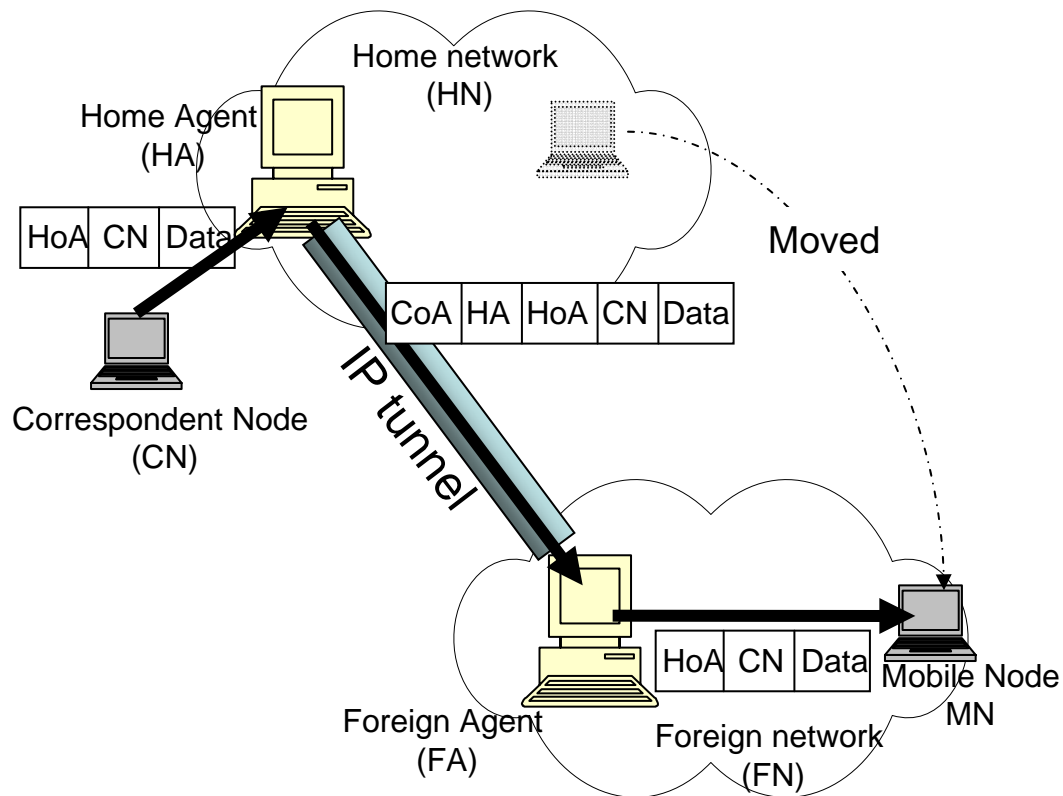


3. Proposal

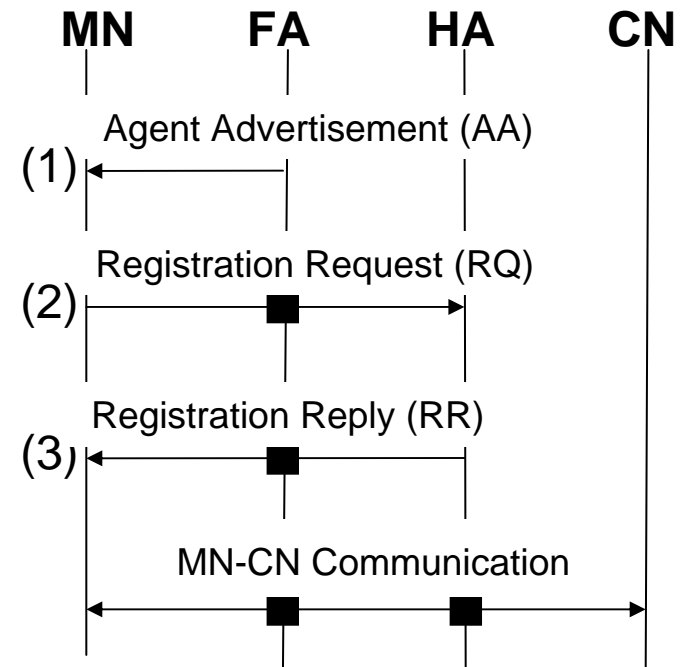
- The proposal is based on **Mobile IP (MIP)**
 - Why Mobile IP?
 - 3GPP2 MIP is used in 3G cellular network. This architecture is similar to our object.
 - Layer 3 access to corporate network and layer 2 access to carrier can be unified by FA-mode Mobile IP
 - Other problems if using MIP for Wide area Ethernet:
 - 1. Conflict over IP address
 - 2. Security inside the Ethernet
 - 3. Efficient multicast
- 2 proposed methods: **MIP+PPPoE** and **MIP+VLAN**

3. FA-mode Mobile IP (MIPv4)

- Two IPv6 version of MIP (MIPv6 and NEMO) are not suitable



MIPv4 architecture



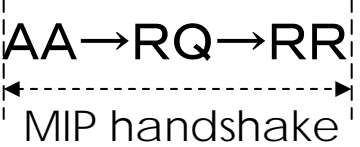
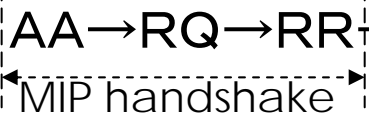
Operating of MIPv4

4.1 MIP+PPPoE

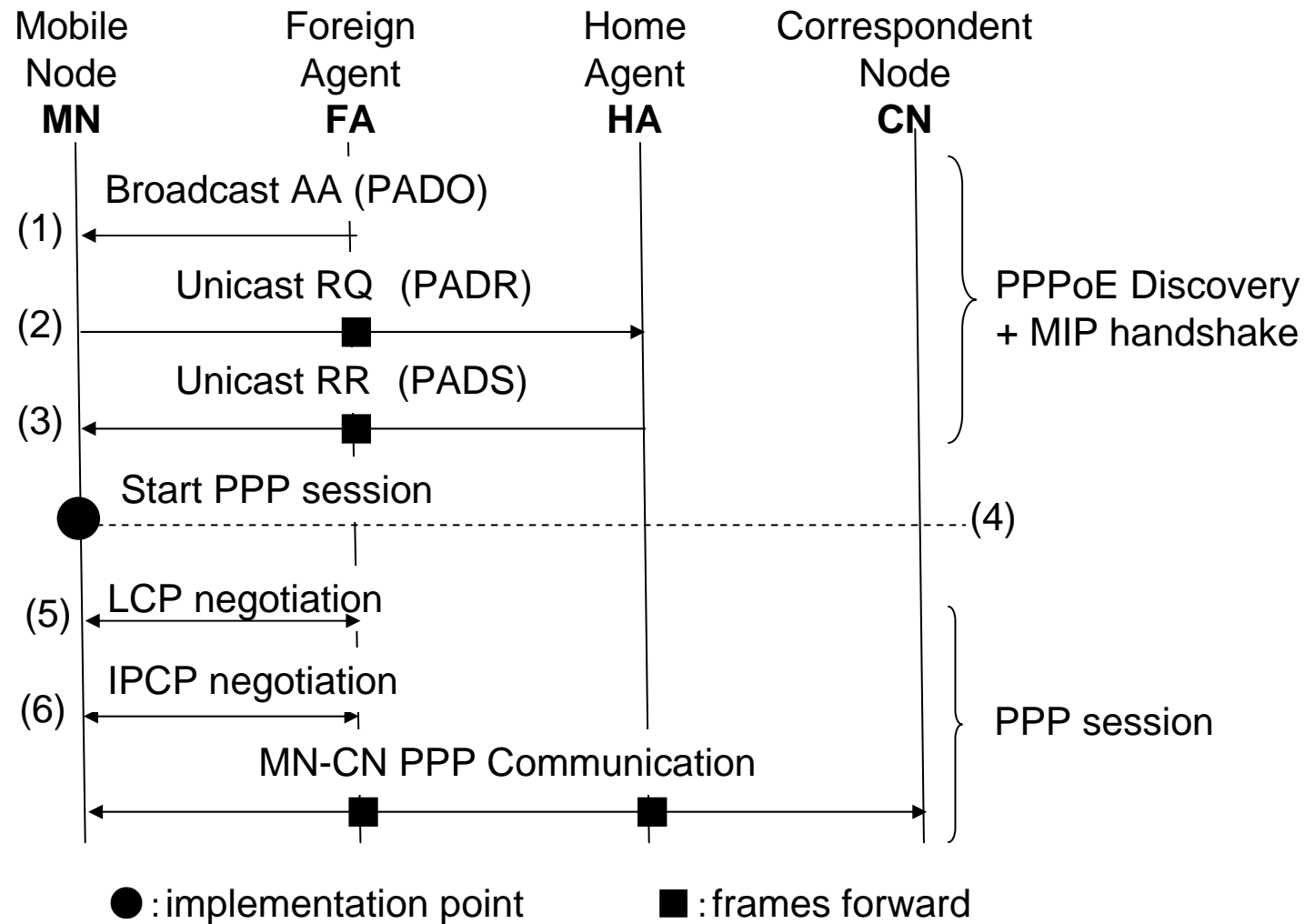
- Problems solved by 3GPP2 MIP(FA=PPPoE server) used for Wide area Ethernet:
 - IP address conflict problem can be solved. ARP is not used.
 - Security in the Ethernet: communication between MN and FA is through PPPoE session.
- Other disadvantages if original 3GPP2 MIP is used for Wide area Ethernet:
 - Large bandwidth is needed to unicast AA frame to all MNs through PPP session.
 - MN uses PPPoE at HN, multicast cannot be used at HN.

4.1 Implementation of MIP+PPPoE

- The difference of MIP+PPPoE from 3GPP2 MIP:
 - MN uses ARP at HN as normal and uses PPPoE at FN
 - MIP handshake is unified with PPPoE Discovery stage.
 - MN receives broadcast frame AA before starting PPP session.
 - After specified time of PPPoE session idle, MN terminates the PPP session and changes to normal ARP.

3GPP2 MIP for Ethernet	PPPoE Discovery → PPPoE Login → AA → RQ → RR <div style="text-align: right; margin-right: 20px;">  </div>
MIP+PPPoE	AA → RQ → RR → PPPoE Login <div style="text-align: left; margin-left: 20px;">  </div>

4.1 Operating of MIP+PPPoE



4.2 MIP+VLAN

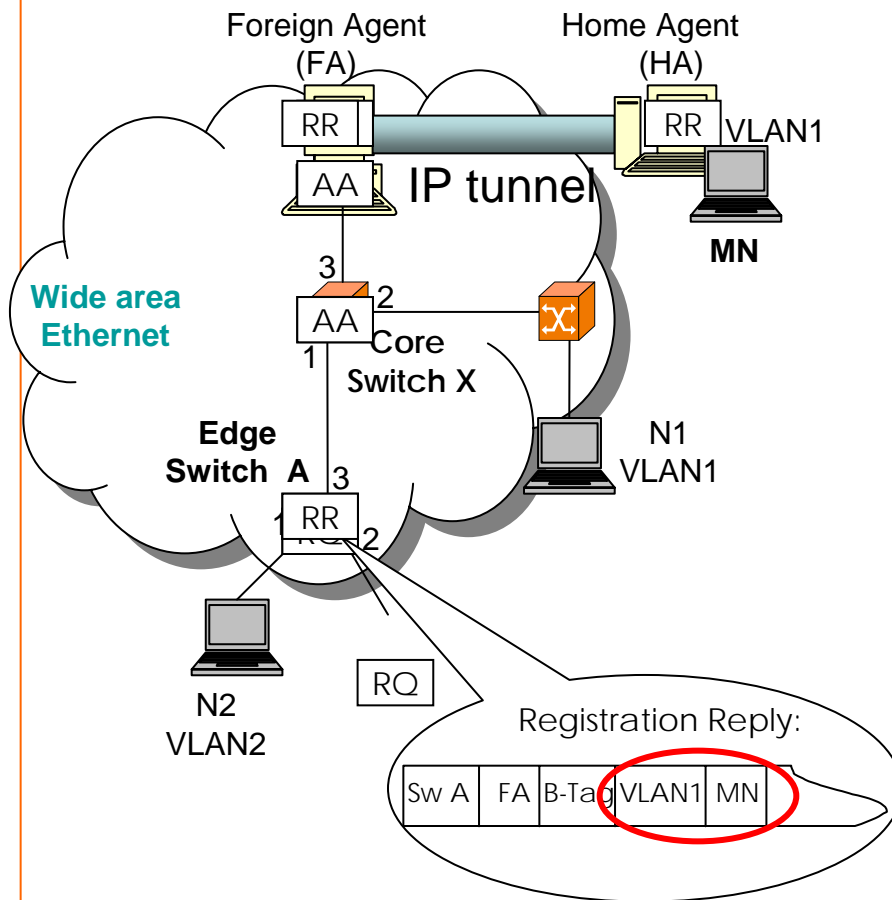
- MIP+PPPoE cannot support multicast among the group of MNs from a same HN.
- VLAN can be used to divide the Wide area Ethernet into logical networks.
- MIP+VLAN:
 - Edge switch automatically learns the VLAN of MN, which is corresponded to its HN
 - Edge switch tags the I-tag to all frames sent by MN

IEEE 802.1ah Ethernet frame format



4.2 Implementation of MIP+VLAN

Static setup :



VLAN table of SW X

VLAN	1	2	3
VLAN0	1	1	1	1
VLAN1	1	1	1	1
VLAN2	1	1	1	1
...				

Port-VLAN table of SW A

VLAN	1	2	3
VLAN0	1	1	1	1

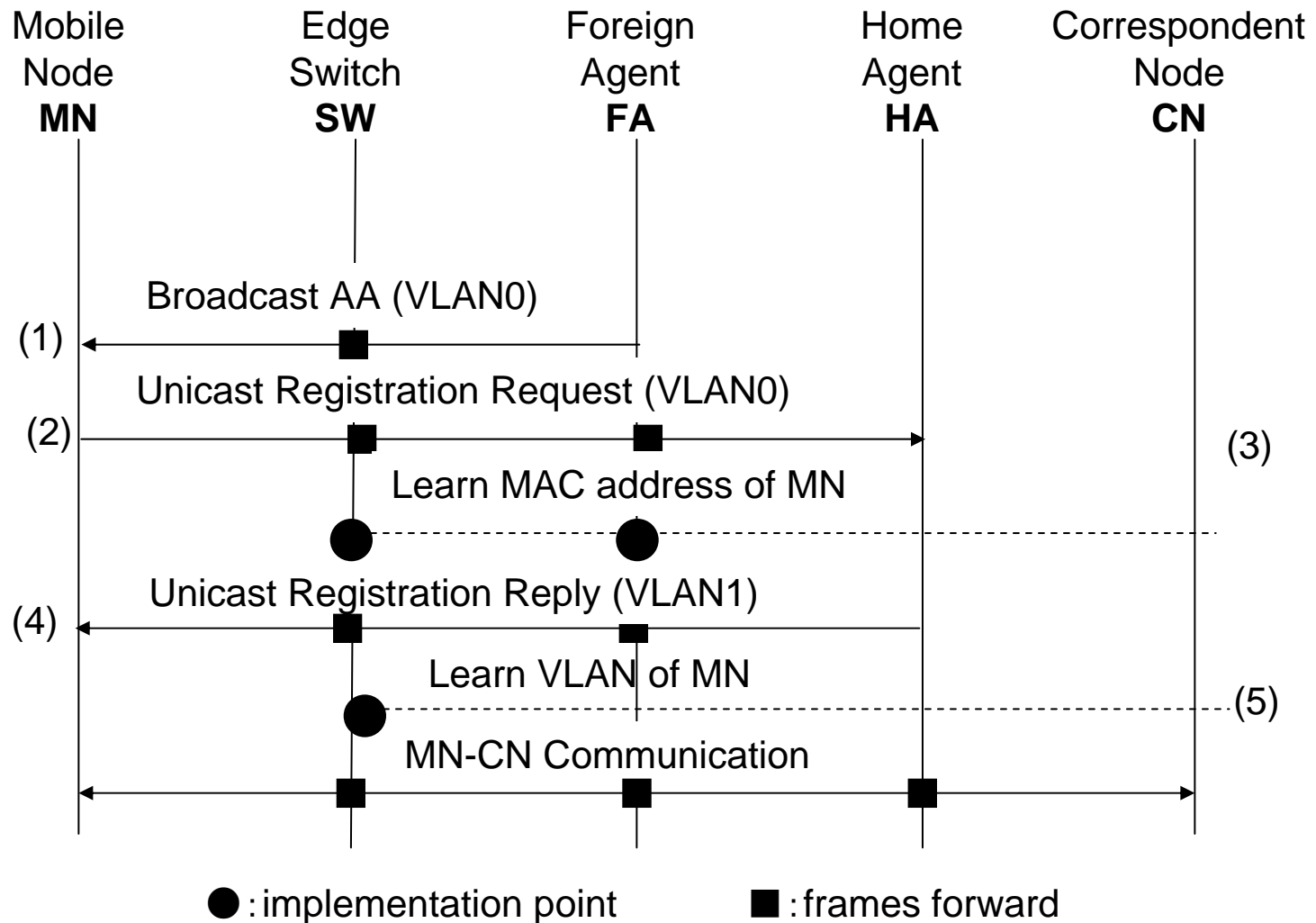
VLAN0 is used for VLAN handshake

Dynamic setup :

MAC address – VLAN table of SW A

MAC-address	VLAN
MAC-N2	VLAN2
MAC-MN	VLAN0
...	

4.2 Operating of MIP+VLAN



4.2 MIP+VLAN messages' frame

Agent Advertisement (AA): FA → every MN, FA tags VLAN0

ff.ff.ff. ff.ff.ff	MAC-FA	B-TAG	VLAN0	ff.ff.ff. ff.ff.ff	MAC-FA		Len/ Type	Agent Advertisement	FCS
-----------------------	--------	-------	-------	-----------------------	--------	--	--------------	------------------------	-----

Registration Request (RQ): MN → FA, SW A tags VLAN0

MAC-FA	MAC -Sw A	B-TAG	VLAN0	MAC-FA	MAC-MN		Len/ Type	Registration Request	FCS
--------	--------------	-------	-------	--------	--------	--	--------------	-------------------------	-----

Registration Reply (RR) : FA → MN, FA tags VLAN1, SW A learns VLAN1

MAC- Sw A	MAC-FA	B-TAG	VLAN1	MAC-MN	MAC-FA	C-TAG optional	Len/ Type	Registration Reply	FCS
--------------	--------	-------	-------	--------	--------	-------------------	--------------	-----------------------	-----

User data frame: MN → CN, SW A tags VLAN1

FA Or Sw B	MAC- Sw A	B-TAG	VLAN1	MAC-CN	MAC-MN	C-TAG optional	Len/ Type	Data	FCS
------------------	--------------	-------	-------	--------	--------	-------------------	--------------	------	-----

4.2 Problems solved by MIP+VLAN

- IP address conflict problem can be solved. MNs from different HN are divided into different VLAN group.
- Security in the Ethernet: 2 ways for an attacker to join the VLAN of MN
 - A) Cheating in the VLAN handshake:
 - > VLAN handshake is unified with MIP handshake. Access challenge responsibility is on the corporate network.
 - B) Replacing MN with an other device after the VLAN handshake
 - > MAC-VLAN mode of edge switch is used
- Multicast: can be used in each VLAN group.

5. Qualitative evaluation

Evaluation index	PPP+VPN	MIP+PPPoE	MIP+VLAN
1. Unify the administration domain -> better security	×	○	○
2. Unify the access authentication -> easier remote access	×	○	○
3. Group multicast	×	×	○
4. No new protocol for MN		×	○
5. No new function for edge switch		○	×

○ : yes × : no

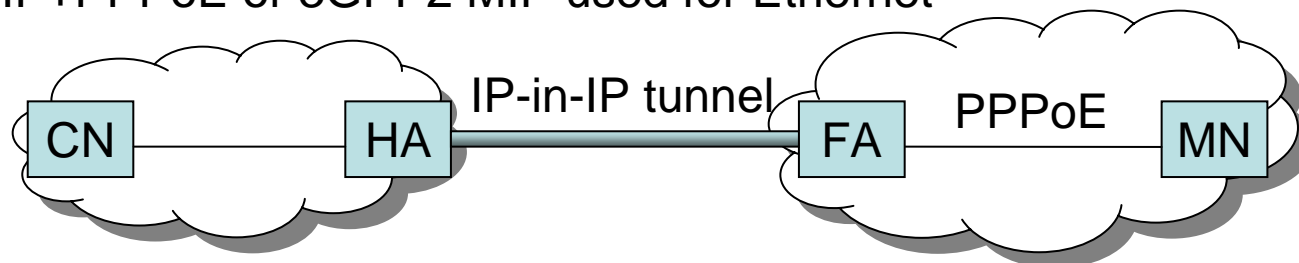
5. Implementation cost

- FA is made by extending function of BAS.
- The operating of methods need to be standardized.
- MIP+PPPoE:
 - MIP handshake frames are in ICMP format. PPPoE Discovery frames are in PPPoE format.
 - > High implementation cost for making a new protocol.
- MIP+VLAN:
 - Original MIPv4 protocol can be used together with IEEE802.1ah.
 - VLAN automatic learning function can be easily implemented to switches by a remote server.
 - > Low implementation cost.

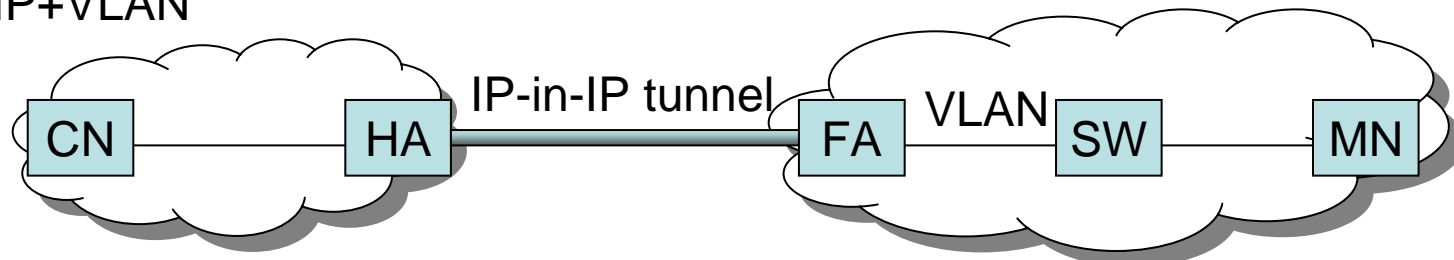
5. Quantitative evaluation

- Quantitative evaluation of access delay:
 - MIPv4 handshake and VLAN: use Qualnet simulator
 - PPPoE: measured by Linux's rp-PPPoE software

a) MIP+PPPoE or 3GPP2 MIP used for Ethernet






b) MIP+VLAN



5. Quantitative evaluation

- Calculated access delay for each method
 - AA time interval is set to be 1 sec in Qualnet simulation

Method	Each access step and delay (millisecond)			Access delay (millisecond)
3GPP2 MIP for Ethernet	PPPoE discovery	PPPoE login	MIP handshake	2028.79 
	5.14	1013.79	1009.86	
MIP+PPPoE	PPPoE discovery & MIP hs	PPPoE login		2022.58 
	1010.44	1012.14		
MIP+VLAN	MIP&VLAN handshake			1013.11 
	1013.11			

Conclusion

- Purpose: Overlay private IP address networks over Wide area Ethernet with low management cost.
- Two proposed methods based on FA-mode Mobile IP:
 - MIP+PPPoE
 - MIP+VLAN
- MIP+VLAN has more advantages
- Future works:
 - Layer 2 encryption and wireless security.
 - Scalability for the Wide area Ethernet service which supports mobility of devices.

Thank you for your attention !